IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

ALAIN LAPTER, ANA LAPTER, STACEY J. P. ULLMAN, MICHAEL SLYNE, JENNIFER PASCUCCI DEMARCO, DANIEL DEMARCO, JR. and PAMELA KLEIN, Individually and on Behalf of all Others Similarly Situated, Plaintiffs, vs. EQUIFAX, INC, Defendant.	**Civil Action No. _____** **COMPLAINT** **CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiffs Alain Lapter, Ana Lapter, Stacey J. P. Ullman, Michael Slyne, Jennifer Pascucci DeMarco, Daniel DeMarco, Jr., and Pamela Klein ("Plaintiffs"), by and through their undersigned counsel, submit this Complaint on behalf of themselves and all others similarly situated. Plaintiffs' allegations are based upon their personal knowledge as to themselves and their own acts, and upon information and belief, developed from the investigation and analysis by Plaintiffs' counsel, including a review of publicly available information.

NATURE OF THE ACTION

1. Defendant Equifax, Inc. ("Equifax" or the "Company"), is a global provider of information solutions and human resources business process outsourcing services for businesses, governments and consumers. The Company operates in four segments: U.S. Information Solutions (USIS), International, Workforce Solutions and Global Consumer Solutions. Its products and services are based on databases of consumer and business information derived from various sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data.

2. As part of its products and services, Equifax collects, stores and transmits its Class members' personal and proprietary information in their facilities and on its equipment, networks and corporate systems. Indeed, before the information complained of herein, Equifax's website stated:

> For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.
>
> We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of

> information, both online and offline, is a top priority for Equifax[1]

3. Equifax did not, however, "protect the privacy and confidentiality of personal information about consumers." On September 7, 2017, Equifax "issued a press release providing important information regarding a cybersecurity incident involving access to certain consumer information" (the "Breach") which press release stated:

> Equifax Inc. (NYSE: EFX) today announced a cybersecurity incident potentially impacting approximately ***143 million U.S. consumers***. Criminals exploited a U.S. website application vulnerability to gain access to certain files. Based on the company's investigation, the unauthorized access occurred from mid-May through July 2017. The company has found no evidence of unauthorized activity on Equifax's core consumer or commercial credit reporting databases.
>
> The information accessed primarily includes ***names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed***. . . .
>
> Equifax discovered the unauthorized access on July 29 of this year and acted immediately to stop the intrusion. The company promptly engaged a leading, independent

[1] *See* https://web.archive.org/web/20170331195307/https://www.equifax.com/privacy.

Emphasis throughout this Complaint is added unless otherwise noted.

cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.com or contact a dedicated call center at 866-447-7559, which the

> company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. - 1:00 a.m. Eastern time.

4. According to a September 8, 2017, *TheStreet.com* article regarding the Breach:[2]

> The breach of the records of 143 million consumers from Equifax[,] one of the three main credit rating bureaus, will increase the opportunity for identity theft to occur since personal information was stolen by hackers.
>
> * * *
>
> This cyberattack has widespread ramifications, since Equifax has "the data on almost everybody in the country," said Jeff Golding, chief growth officer at IRH Capital, a Northbrook, Ill.-based financial company and former CEO of WilliamPaid, a company that allows people to build credit through paying their rent online. The U.S. Census Bureau estimated in its 2015 survey that there are 321 million people living in the U.S.
>
> The three main credit bureaus, Equifax, TransUnion and Experian, maintain reports on when consumers' attempt to obtain loans, their payment history and the amount of available credit. Lenders use one or all three of these companies when consumers seek a credit card, mortgage or other loans.
>
> "This is a big deal," Golding said. "If you ever had your credit pulled, they have information on you. If you ever filled out a loan application, they will have data like your driver's license."

[2] *See* https://www.thestreet.com/story/14298348/1/equifax-breach-of-143-million-consumers-increases-identity-theft-odds.html

The data breach of Equifax data breach could "potentially be one of the most significant data breaches in history," said Marie White, CEO of Security Mentor, a Pacific Grove, Calif.-based provider of security awareness training.

"The size of the breach, quality and quantity of personal information and far-reaching impact make it unprecedented," she said. "Imagine if one out of every two people walking down the street dropped their credit card, along with a sticky note on the back with all their personal information needed to access that card. Now imagine that happening in every city across the county."

* * *

"Experian also sells background check services and identity theft service which they monitor daily," he said. "Their databases house all your personal data that's ever been provided, acquired though applications, lenders they work with or credit card companies. They are constantly buying data back and forth."

While not all lenders report to all three bureaus, consumers who applied for a mortgage are likely to have their scores pulled for all of the companies. Consumers who use Credit Karma or Credit Sesame or credit card companies such as Chase or Discover to monitor their credit score will see different scores since some lenders report to one while others report to two or all three.

"Your credit profiles can be different," Golding said. "Lenders aren't required to report data. It's elective and they do it as self-policing their industry."

Since the hackers have copious amounts of personal identifiable information, your identity could likely be compromised, he said.

> "This makes it a lot easier for identity theft to occur," but it is unlikely that the hackers gained access to all their encrypted databases to match up all the information such as the driver's license or Social Security number, Golding said.
>
> While Equifax has not revealed the specifics of the hack, ***either the databases were not encrypted or the "application vulnerability that was exploited provided authorized access to the data in an unencrypted state,"*** said Nathan Wenzler, chief security strategist at AsTech, a San Francisco-based security consulting company.
>
> When databases are stolen whole, companies have announced that they don't believe the information can be accessed, but are providing free credit monitoring services just as a precaution.
>
> "***For Equifax to come out and state what data was actually lost and to not include any statement like that suggests that the data itself was actually compromised," he said. "Either because it wasn't encrypted at all, or the exploit granted authorized access to decrypt the data and provide it to the attacker as a valid request***. I am not sure if we'll ever see that level of detail come from Equifax and their investigation, though, which confirms the specific exploits or how the data was, or was not, encrypted."

5. Plaintiffs and other members of the Class and Subclasses, defined below, are now forced to incur out-of-pocket expenses and to take steps (including freezing their credit files) to protect themselves from, or to remediate harm caused by, identity thieves and other criminals.

6. Plaintiffs bring this action as a class action against Equifax for its negligent failure to adequately protect the personal information of the Class and for failing to timely notify the Class that their personal information had been stolen from Equifax's computer system. Plaintiffs seek to recover damages caused to her and the Class and Subclasses caused by Equifax's violations of law. Plaintiffs seek injunctive relief requiring Equifax to properly safeguard the Class's personal information on its computer system or alternatively, remove such personal information from its computer system.

PARTIES

7. Plaintiff Alain Lapter's data was compromised as a result of the Breach. He is a resident of the state of Virginia.

8. Plaintiff Ana Lapter's data was compromised as a result of the Breach. She is a resident of the state of Virginia.

9. Plaintiff Stacey J. P. Ullman's data was compromised as a result of the Breach. She is a resident of the state of New Jersey.

10. Plaintiff Michael Slyne's data was compromised as a result of the Breach. He is a resident of the state of Connecticut.

11. Plaintiff Jennifer Pascucci DeMarco's data was compromised as a result of the Breach. She is a resident of the state of Pennsylvania.

12. Plaintiff Daniel DeMarco, Jr.'s data was compromised as a result of the Breach. He is a resident of the state of Pennsylvania.

13. Plaintiff Pamela Klein's data was compromised as a result of the Breach. She is a resident of the state of New York.

14. Defendant Equifax is organized under the laws of the state of Georgia and maintains its principal executive offices at 1550 Peachtree Street, N.W., Atlanta, Georgia 30309. In public filings with the Securities and Exchange Commission, Equifax describes its business as "a leading global provider of information solutions, employment and income verifications and human resources business process outsourcing services" that "leverage[s] some of the largest sources of consumer and commercial data, along with advanced analytics and proprietary technology, to create customized insights which enable our business customers to grow faster, more efficiently and more profitably, and to inform and empower consumers."

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs and defendant

Equifax are citizens of different states. The proposed Class and Subclasses each include well over 100 members.

16. This Court has jurisdiction over Equifax because the Company maintains its principal place of business in this District in Atlanta; regularly conducts business in Georgia; and has sufficient minimum contacts in Georgia. Equifax intentionally avails itself of this jurisdiction by marketing and selling products from Georgia to millions of consumers nationwide, including in the state of New York.

17. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Equifax is a resident of this District and is subject to this Court's personal jurisdiction. Equifax is incorporated in Georgia, regularly conducts business in this District, and maintains its headquarters in this District. In addition, the causes of action arose, in substantial part, in this District.

CLASS ACTION ALLEGATIONS

18. Plaintiffs bring this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of themselves and all others similarly situated in the United States, who, as a result of the Breach, had their personal information stolen from Equifax computer systems, and were damaged thereby (the "Class"). Plaintiffs also brings Count III alleged below on behalf of a

subclasses of Virginia, New Jersey, Connecticut and New York residents for whom Equifax gathered personal information during and since the Breach and had their personal information stolen from Equifax computer systems and were damaged thereby (the "Subclasses"). The Class and Subclasses do not include Defendants' officers, agents, and employees.

19. The Class and Subclasses consist of potentially millions of persons for whom Equifax collected personal information. While the exact number of members of the Class and Subclasses and the identities of individual members of the Class and Subclass are unknown to Plaintiffs' counsel at this time, and can only be ascertained through appropriate discovery, based on the fact that 143 million persons for whom Equifax collected personal information have been adversely affected, the membership of the Class and Subclass are each so numerous that joinder of all members is impracticable.

20. Equifax's wrongful conduct affected all members of the Class and Subclass in exactly the same way. The Defendant's failure to properly safeguard the Class's personal information is completely uniform among the Class and Subclasses.

21. Questions of law and fact common to all members of the Class and Subclasses predominate over any questions affecting only individual members. Such common questions of law and fact include:

a. whether the Defendant acted wrongfully by failing to properly safeguard personal information persons for whom Equifax collected personal information on its computer system;

b. whether Defendant's conduct violated law;

c. whether the Plaintiffs and the other members of the Class and Subclasses have been damaged, and, if so, what is the appropriate relief; and

d. whether the Defendant breached its duties owed to members of the Class and Subclasses and by failing to properly safeguard their personal information.

22. The Plaintiffs' claims, as described herein, are typical of the claims of all other members of the Class and Subclasses, as the claims of the Plaintiffs and all other members of the Class and Subclasses arise from the same set of facts regarding the Defendant's failure to protect the Class and Subclasses member's personal information from computer hackers. The Plaintiffs maintain no interest antagonistic to the interests of other members of the Class or Subclasses.

23. The Plaintiffs are committed to the vigorous prosecution of this action and has retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, the Plaintiffs are adequate representatives of the Class and Subclasses and will fairly and adequately protect their interests.

24. This class action is a fair and efficient method of adjudicating the claims of the Plaintiffs and the Class and Subclasses for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class and Subclasses' members;

b. the prosecution of separate actions by individual Class and Subclasses' members would likely create a risk of inconsistent or varying adjudications with respect to individual members thereby establishing incompatible standards of conduct for Defendant or would allow some Class and Subclasses' members' claims to adversely affect the ability of other members to protect their interests;

c. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District;

d. the Plaintiffs anticipate no difficulty in the management of this litigation as a class action; and

e. the Class and Subclasses are readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

25. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

SUBSTANTIVE ALLEGATIONS

26. Plaintiffs are among the hundreds of millions of Americans who have applied for a loan or had their credit pulled for one reason or another, and thus for whom Equifax has complied sensitive and confidential personal information.

27. Equifax collected and stored Plaintiffs' personal information on its computer system and used that information for, among other things, profit.

28. On September 7, 2017, Equifax issued a press release announcing "a cybersecurity incident potentially impacting approximately ***143 million U.S. consumers.***" *See supra* ¶ 3.

29. The Breach apparently occurred from mid-May through July 2017, and Equifax apparently learned of the breach Equifax discovered the unauthorized access on July 29, 2017, forty days before the Breach was disclosed.

30. Even after forty days, Equifax's disclosure of the Breach was woefully deficient. As reported by *Tech Crunch*,

> Equifax just announced a massive data breach that could affect 143 million consumers. It's shaping up to be one of the largest hacks of all time. The information came mostly from U.S. residents, but a percentage also involved U.K. and Canadian citizens and the company is working with authorities from these countries.
>
> The company established a website to allow consumers to see if their data was stolen. But it's broken and sets the user up for TrustedID, a credit monitoring service owned by, wait for it, Equifax.
>
> Equifax says that this site will "indicate whether your personal information may have been impacted by this incident." That is false as of this post's publication. The company also says it will provide the checker with an "option" to enroll in TrustedID Premier. That's also false. When a user inputs their data into the system, a message appears that the user can be enrolled in TrustedID Premier at a later date. Mine was 9/11/2017.
>
> This is completely irresponsible by Equifax.
>
> The site's terms of service seem to state that by agreeing to use this service, the user is waving their rights to bring a class action lawsuit against Equifax.
>
> We have a note out to the company asking for clarification about this site's capabilities, function and any rights forfeited. Until questions are answered, I would avoid using the site.
>
> This is essentially the site right now.
>
> …

EQUIFAX: we may have leaked your SSN

ALSO EQUIFAX: give us your SSN to see if we leaked it

COUNTS

FIRST CAUSE OF ACTION

Negligence

31. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

32. Equifax owed a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting personal information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Equifax's computer network security systems to ensure that Plaintiffs and the other members of the Class' personal information in Equifax's possession were adequately secured and protected. Equifax further owed a duty to Plaintiffs and the other members of the Class to implement processes that would timely detect a breach of its computer security and to prevent mass exports of personal information out of Equifax's computer network.

33. Equifax owed a duty of care to Plaintiffs and the other members of the Class and Subclasses because there was a reasonable expectation that Equifax

would keep that information secure and confidential. Equifax solicited, gathered, and stored the personal information for its own business purposes. Equifax, in the absence of negligence, would have known by holding massive amounts of personal information it was a lucrative target for hackers and a breach of its computer security systems and the stealing of personal data would damage to Plaintiffs and the other members of the Class. Equifax had a duty to adequately protect such the Class's personal information from hackers.

34. Plaintiffs and other members of the Class relied on Equifax to safeguard their personal information that it collected, used and stored and was in a position to (and capable of) protecting against the harm caused to Plaintiffs and the other members of the Class as a result of the Breach.

35. Equifax's conduct created a foreseeable risk of harm to Plaintiffs and the other members of the Class. Equifax's misconduct included, but was not limited to, its failure to take the steps and opportunities to effectively encrypt, and then to prevent and stop the Breach, and to timely detect and disclose the Breach as set forth herein.

36. Equifax breached the duties it owed to Plaintiffs and the other members of the Class by failing to exercise reasonable care and implement

adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiffs and the other members of the Class.

37. Equifax breached the duties it owed to Plaintiffs and the other members of the Class by failing to properly implement technical systems or security practices that could have prevented the loss of the confidential data at issue.

38. Plaintiffs and the other members of the Class were damaged by Equifax's breach of this duty as a direct and proximate result of Equifax's conduct suffered damages including, but not limited to, loss of control of their personal information, an added burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

SECOND CAUSE OF ACTION

Unjust Enrichment

39. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

40. Plaintiffs and members of the Class or, alternatively, the Subclasses (collectively, the "Class" as used in this Count), had their personal information

collected and sold by Equifax. That information conferred a monetary benefit on Equifax.

41. Equifax knew that Plaintiffs' and the Class's information conferred a benefit on Equifax, which profited by using their Personal Information for its own business purposes.

42. Equifax failed to secure the Plaintiffs' and Class members' personal information, and acquired the personal information through inequitable means because it failed to disclose the inadequate security practices previously alleged.

43. Had Plaintiffs and Class members known that Equifax would not secure their personal information using adequate security, they would have requested Equifax destroy or not retain such information.

44. Plaintiffs and the Class have no adequate remedy at law.

45. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits that Plaintiffs and Class members' personal information conferred on it.

46. Equifax should be compelled to disgorge into a common fund or constructive trust for the benefit of the proceeds it received from processing and selling Plaintiffs and Class members' personal information.

THIRD CAUSE OF ACTION

Declaratory Judgment

47. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

48. As previously alleged, Equifax owed duties of care to Plaintiffs and the members of the Class or, alternatively, the Subclasses, that require it to adequately secure personal information.

49. Equifax still possesses Personal Information regarding the Plaintiffs' and the Class members.

50. After the Breach, Equifax announced changes that it claimed would improve data security. These changes, however, did not fix many systemic vulnerabilities in Equifax's computer systems. An "FAQ" posted to https://www.equifaxsecurity2017.com/frequently-asked-questions/, states that "to prevent this from happening again" Equifax has "engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again."

51. Accordingly, Equifax still has not satisfied its obligations and legal duties to Plaintiffs and the Class members.

52. Actual harm has arisen in the wake of Equifax's data breach regarding its obligations and duties of care to provide security measures to Plaintiffs and the members of the Class and Subclasses. Equifax does not maintain that its security measures now are adequate to meet Equifax's contractual obligations and legal duties.

53. Plaintiffs, therefore, seek a declaration (a) that Equifax's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (b) that to comply with its obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to: (1) ordering that Equifax engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors; (2) ordering that Equifax engage third-party security auditors and internal personnel to run automated security monitoring; (3) ordering that Equifax audit, test, and train its security personnel regarding any new or modified procedures; (4) ordering that Equifax segment Class members' data by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other

portions of Equifax's systems; (5) ordering that Equifax purge, delete, and destroy in a reasonably secure manner Class members' data not necessary for its provisions of services; (6) ordering that Equifax conduct regular database scanning and securing checks; and (7) ordering that Equifax routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

FOURTH CAUSE OF ACTION

Violation of the Virginia Data Breach Act

(On Behalf of the Virginia Subclass only)

54. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiffs Alain Lapter and Ana Lapter and the other members of the Virginia Subclass are Class members whose personal information Equifax used for personal and private use.

55. By failing to timely notify the Virginia Subclass of the data breach, Equifax violated Section 18.2-186.6 of the Code of Virginia, which provides, in part:

> B. If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or

> will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

56. The Breach constituted a "Breach of the security of the system" of Equifax within the meaning of the above Virginia data breach statute and the data breached was protected and covered by the data breach statute.

57. Equifax unreasonably delayed informing the public, including Plaintiffs and the members of the Virginia Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

58. Equifax failed to disclose the Breach reach to Plaintiffs and the other members of the Virginia Subclass without unreasonable delay and in the most expedient time possible.

59. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiffs and the other members of the Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

60. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiffs and the other members of the Virginia Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiffs and the other members of the Virginia Subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiffs and the Subclass members could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

FIFTH CAUSE OF ACTION

Violation of the New Jersey Data Breach Act

(On Behalf of the New Jersey Subclass only)

61. Plaintiffs incorporate and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff Stacey J. P. Ullman and the other members of the New Jersey Subclass are Class members whose personal information Equifax used for personal and private use.

62. By failing to timely notify the New Jersey Subclass of the data breach, Equifax violated N.J.S.A. 56:8-163, which provides, in part:

> a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.

> b. Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records immediately following discovery, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.
>
> c. (1) Any business or public entity required under this section to disclose a breach of security of a customer's personal information shall, in advance of the disclosure to the customer, report the breach of security and any information pertaining to the breach to the Division of State Police in the Department of Law and Public Safety for investigation or handling, which may include dissemination or referral to other appropriate law enforcement entities.
>
> (2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.

63. The Breach constituted a "Breach of security" of Equifax within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

64. Equifax unreasonably delayed informing the public, including Plaintiff and the members of the Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

65. Equifax failed to disclose the Breach reach to Plaintiff and the other members of the Subclass without unreasonable delay and in the most expedient time possible.

66. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiff and the other members of the Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

67. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff and the other members of the New Jersey Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiff and the other members of the Subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiff and the Subclass members could have avoided providing further data to Equifax, could have

avoided use of Equifax's services, and could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

SIXTH CAUSE OF ACTION

Violation of the Connecticut Data Breach Act

(On Behalf of the Connecticut Subclass only)

68. Plaintiffs incorporate and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff Michael Slyne and the other members of the Connecticut Subclass are Class members whose personal information Equifax used for personal and private use.

69. By failing to timely notify the Connecticut Subclass of the data breach, Equifax violated Connecticut's data security law, § 36a-701b, which provides, in part:

> (b) (1) Any person who conducts business in this state, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information, shall provide notice of any breach of security following the discovery of the breach to any resident of this state whose personal information was breached or is reasonably believed to have been breached. Such notice shall be made without unreasonable delay but not later than ninety days after the discovery of such breach, unless a shorter time is required under federal law, subject to the provisions of subsection (d) of this section and the completion of an investigation by such person to determine the nature and scope of the incident, to identify the individuals affected,

> or to restore the reasonable integrity of the data system. Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed.
>
> * * *
>
> (d) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.

70. Equifax unreasonably delayed informing the public, including Plaintiff and the members of the Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

71. Equifax failed to disclose the Breach reach to Plaintiff and the other members of the Subclass without unreasonable delay and in the most expedient time possible.

72. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiff and the other members of the

Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

73. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff and the other members of the Connecticut Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiff and the other members of the Subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiff and the Subclass members could have avoided providing further data to Equifax, could have avoided use of Equifax's services, and could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

SEVENTH CAUSE OF ACTION

Violation of the Pennsylvania Data Breach Act

(On Behalf of the Pennsylvania Subclass only)

74. Plaintiffs incorporate and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiffs Jennifer Pascucci DeMarco and Daniel DeMarco, Jr. and the other members of the Pennsylvania

Subclass are Class members whose personal information Equifax used for personal and private use.

75. By failing to timely notify the Pennsylvania Subclass of the data breach, Equifax violated Chapter 43, Section 2303 of Pennsylvania's Breach of Personal Information Notification Act, which provides, in part:

> **(a) General rule.--**An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4[1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
> **(b) Encrypted information.--**An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

76. The Breach constituted a "Breach of the security of the system" of Equifax within the meaning of the above Pennsylvania data breach statute and the data breached was protected and covered by the data breach statute.

77. Equifax unreasonably delayed informing the public, including Plaintiffs and the members of the Pennsylvania Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

78. Equifax failed to disclose the Breach reach to Plaintiffs and the other members of the Pennsylvania Subclass without unreasonable delay and in the most expedient time possible.

79. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiffs and the other members of the Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

80. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiffs and the other members of the Pennsylvania Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiffs and the other members of the Pennsylvania Subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiffs and the Subclass members could have avoided providing further data to Equifax, could

have avoided use of Equifax's services, and could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

EIGHTH CAUSE OF ACTION

Violation of the New York Data Breach Act

(On Behalf of the New York Subclass only)

81. Plaintiffs incorporate and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein. Plaintiff Pamela Klein and the other members of the New York Subclass are Class members whose personal information Equifax used for personal and private use.

82. By failing to timely notify the New York Subclass of the data breach, Equifax violated GBS § 899-aa, which provides, in part:

> 2. Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision four of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.

* * *

> 4. The notification required by this section may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. The notification required by this section shall be made after such law enforcement agency determines that such notification does not compromise such investigation.
>
> * * *
>
> 7. Regardless of the method by which notice is provided, such notice shall include contact information for the person or business making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so acquired.

83. Further, New York law provides that "in addition to any other lawful remedy" "Whenever the court shall determine in such action that a person or business violated this article knowingly or recklessly, the court may impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, provided that the latter amount shall not exceed one hundred fifty thousand dollars. "

84. The Breach constituted a "Breach of the security of the system" of Equifax within the meaning of the above New York data breach statute and the data breached was protected and covered by the data breach statute.

85. Equifax unreasonably delayed informing the public, including Plaintiff and the members of the Subclass, about the data breach after Equifax knew or should have known that the data breach had occurred.

86. Equifax failed to disclose the Breach reach to Plaintiff and the other members of the Subclass without unreasonable delay and in the most expedient time possible.

87. Equifax has provided no indication that any law enforcement agency requested that Equifax delay notification. Plaintiff and the other members of the Subclass suffered harm directly resulting from Equifax's failure to provide and the delay in providing notification of the Breach with timely and accurate notice as required by law.

88. As a result of said practices, Equifax has directly, foreseeably, and proximately caused damages to Plaintiff and the other members of the New York Subclass. Had Equifax provided timely and accurate notice of the Breach Plaintiff and the other members of the Subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Equifax in providing notice. Plaintiff and the Subclass members could have avoided providing further data to Equifax, could have

avoided use of Equifax's services, and could otherwise have tried to avoid the harm caused by Equifax's delay in providing timely and accurate notice.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully request that this Court:

A. Certify this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiffs as Class and Subclass representatives and their counsel as Class counsel;

B. Award Plaintiffs and the other members of the Class and Subclass appropriate relief, including actual and statutory damages;

C. Enter judgment in favor of Plaintiffs and the other members of the Class and against the Defendant under the legal theories alleged herein;

D. Award reasonable attorneys' fees, costs, and expenses;

E. Award the Plaintiffs and the other members of the Class and Subclass pre-judgment and post-judgment interest at the maximum rate allowable by law;

F. Award Plaintiffs and the other members of the Class and Subclass equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiffs on behalf of the other members of the Class and Subclass seek appropriate injunctive relief designed to ensure against the recurrence of a data

breach by adopting and implementing reasonable data security practices to safeguard Class members' personal information, by an Order requiring Equifax to implement reasonable data security enhancements as they become available, including data encryption, segregation of sensitive data, more robust passwords, authentication of users, increased control of access to sensitive information on the network, prohibitions of mass exports of sensitive data;

G. Enter Declaratory Judgment that the provisions in Equifax's Liability Limit and Choice of Law Provision do not constitute binding agreements and are unconscionable and unenforceable;

H. Enter such additional orders or judgment as may be necessary to prevent a recurrence of the Breach and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint; and

I. Grant such other and further relief as the Court deems just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: September 8, 2017

By: */s/ James M. Evangelista*

James M. Evangelista
Georgia Bar No. 707807
David J. Worley
Georgia Bar No. 776665
Kristi Stahnke McGregor
Georgia Bar No. 674012
EVANGELISTA WORLEY, LLC
8100 A. Roswell Road
Suite 100
Atlanta, GA 30350
Tel: (404) 205-8400
jim@ewlawllc.com
david@ewlawllc.com
kristi@ewlawllc.com

Howard T. Longman
Michael Klein
Melissa Emert
STULL, STULL & BRODY
6 East 45th Street
New York, NY 10017
Tel: (212) 687-7230
Fax: (212) 490-2022
Email:
hlongman@ssbny.com
memert@ssbny.com
mklein@ssbny.com

Counsel for Plaintiffs